

BAB V PENUTUP

5.1 Kesimpulan

Setelah dilakukan penelitian terhadap terkait tingkat keamanan dari website SMK N 1 Pangandaran didapatkan celah SQL Injection terhadap website SMK N 1 Pangandaran dari hasil report analisis yang dilakukan tools ZAP dari OWASP (*Open Web Application Security Project*) terhadap subdomain *cbt.smkn1pangandaran.sch.id* terdapat celah *SQL Injection*. Dimana pada celah tersebut memungkinkan seseorang dengan memanfaatkan SQL Injection untuk masuk kedalam sistem dari *website* melalui subdomain yang ada. Maka dilakukan rekomendasi untuk menutup *bug* ataupun celah yang ada pada *subdomain* *cbt.smkn1pangandaran.sch.id* dengan memanfaatkan proses filter pada saat proses login pada laman tersebut, selain dengan memanfaatkan filter *username* dan *password* juga dengan memanfaatkan *mysql prepare statement* yang menjadi ciri khas dari php versi 7 yang semakin menambah keamanan dari proses login yang ada agar terhindar dari serangan *SQL Injection*.

5.2 Saran

Saran untuk penelitian yang akan datang, semoga dengan adanya penelitian ini dapat memberikan gambaran terkait serangan yang mungkin terjadi pada website maupun subdomain dari website yang ada, yang menjadi pertanda bahwa setiap elemen pada saat proses pembuatan website harus dirancang sebaik mungkin. Pada penelitian ini masih menggunakan metode dan tools yang sederhana, diharapkan penelitian selanjutnya dapat memanfaatkan tools yang lebih baik dan lebih lengkap terkait hasil analisis maupun proses pencarian kelemahan yang ada diharapkan penelitian yang akan dapat menjadi lebih baik.